Reference Manual for the Model RP614 v2 Web Safe Router

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

SM-RP614NA-2
Version 4.12
February 2003

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the Model RP614 v2 Web Safe Router is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Model RP614 v2 Web Safe Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the Model RP614 v2 Web Safe Router has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your Model RP614 v2 Web Safe Router.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Contents

Chapter 6
Troubleshooting

Appendix A
Technical Specifications

Appendix B
Networks, Routing, and Firewall Basics

**Appendix C
Preparing Your Network**

Glossary

Index

Preface
About This Manual

Congratulations on your purchase of the NETGEAR® Model RP614 v2 Web Safe Router.

The RP614 v2 router provides connection for multiple personal computers (PCs) to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single PC.

Audience

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

Typographical Conventions

This guide uses the following typographical conventions:

italics	Media titles, UNIX files, commands, URLs, and directory names.
bold times roman	User input
<u>Internet Protocol</u> (IP)	First time an abbreviated term is used.
`courier font`	Screen text, user-typed command-line entries.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
SMALL CAPS	DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

> **Note:** This format is used to highlight information of importance or special interest.

Chapter 1
Introduction

This chapter describes the features of the NETGEAR Model RP614 v2 Web Safe Router.

Key Features of the Router

The Model RP614 v2 Web Safe Router with 4-port switch connects your <u>local area network</u> (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The RP614 v2 router provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts -- both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. <u>Network Address Translation</u> (NAT) protects you from hackers.

With minimum setup, you can install and use the router within minutes.

The RP614 v2 router provides the following features:

- Easy, web-based setup for installation and management
- Stateful Packet Inspection, Content Filtering, and Site Blocking Security
- Built in 4-port 10/100 Mbps Switch
- Ethernet connection to a <u>wide area network</u> (WAN) device, such as a cable modem or DSL modem
- Extensive Protocol Support
- Login capability
- Front panel LEDs for easy monitoring of status and activity
- Flash memory for firmware upgrade

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the Model RP614 v2 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection.

    Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.

- Blocks unwanted traffic from the Internet to your LAN.

- Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- Logs security incidents.

    The Model RP614 v2 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to email the log to you at specified intervals. You can also configure the router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- With its content filtering feature, the Model RP614 v2 prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Security

The RP614 v2 router is equipped with several features designed to maintain security, as described in this section.

- PCs Hidden by NAT
  NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.

- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated "DMZ" host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink™

With its internal 4-port 10/100 switch, the Model RP614 v2 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a PC or an 'uplink' connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The RP614 v2 router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, "Network, Routing, Firewall, and Basics."

- IP Address Sharing by NAT
  The RP614 v2 router allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached PCs by DHCP
  The RP614 v2 router dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached PCs. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- PPP over Ethernet (PPPoE)
  PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as Entersys or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the Model RP614 v2 Web Safe Router within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Smart Wizard.** The RP614 v2 router automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Visual monitoring.** The RP614 v2 router's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the RP614 v2 router:

- Flash memory for firmware upgrade
- Free technical support seven days a week, twenty-four hours a day

Package Contents

The product package should contain the following items:

- Model RP614 v2 Web Safe Router.
- AC power adapter.
- Category 5 (CAT5) Ethernet cable.
- *Model RP614 v2 Resource CD*, including:
    — This guide.
    — Application Notes and other helpful information.
    — AOL v8.0 client software.
- *RP614 Cable/DSL Web Safe Router Installation Guide.*
- Registration and Warranty Card.
- Support Information Card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the router for repair.

The Router's Front Panel

The front panel of the Model RP614 v2 Web Safe Router (Figure 1-1) contains status LEDs.

Figure 1-1: RP614 Front Panel

You can use some of the LEDs to verify connections. Viewed from left to right, Table 2 describes the LEDs on the front panel of the router. These LEDs are green when lit.

Table 2.   LED Descriptions

Label	Activity	Description
Power	On Off	Power is supplied to the router. Power is not supplied to the router.
Test	On Off	The system is initializing. The system is ready and running.
Internet	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Internet (WAN) port has detected a 100 Mbps link with an attached device. Data is being transmitted or received by the Internet port. The Internet (WAN) port has detected a 10 Mbps link with an attached device. Data is being transmitted or received by the Internet port. The Internet (WAN) port in not connected or the electric power to the device to which it is connected is turned off.
4 Local	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Local (LAN) port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

The Router's Rear Panel

The rear panel of the Model RP614 router (Figure Figure 1-2:) contains port connections.
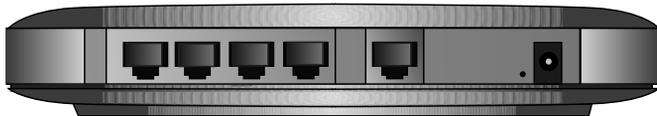
Figure 1-2: RP614 Rear Panel

Viewed from left to right, the rear panel contains the following features:

• Four Local (LAN) Ethernet ports for connecting the router to the local PCs

• Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem

• Factory Default Reset push button

• AC power adapter outlet

Chapter 2
Connecting the Router to the Internet

This chapter describes how to set up the router on your <u>local area network</u> (LAN) and connect to the Internet. You find out how to configure your Model RP614 v2 Web Safe Router for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you begin:

1. Have active Internet service such as that provided by an cable or DSL broadband account.

2. Locate the Internet Service Provider (ISP) configuration information for your DSL account.

3. Connect the router to a cable or DSL modem and a computer as explained below.

Cabling and Computer Hardware Requirements

To use the RP614 v2 router on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your router.

Computer Network Configuration Requirements

The Model RP614 v2 includes a built-in Web Configuration Manager. To access the configuration menus on the Model RP614 v2, your must use a Java-enabled web browser program which supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. NETGEAR recommends using Internet Explorer or Netscape Navigator 4.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

For the initial connection to the Internet and configuration of your router, you will need to connect a computer to the router which is set to automatically get its TCP/IP configuration from the router via DHCP.

Note: For help with DHCP configuration, please refer to Appendix C, "Preparing Your Network".

The cable or DSL modem broadband access device must provide a standard 10 Mbps (10BASE-T) or 100 Mbps (100BASE-TX) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your router to the Internet:

•   Host and Domain Names.

•   ISP Login Name and Password.

•   ISP Domain Name Server (DNS) Addresses.

•   Fixed IP Address which is also known as Static IP Address.

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

•   Your ISP provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.

•   If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.

   — For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.

   — For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.

   — For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.

•   You may also refer to the *Model RP614 v2 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

Worksheet to Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: _____ Password: _____

Service Name: _____

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____ . _____ . _____ . _____
Gateway IP Address: _____ . _____ . _____ . _____
Subnet Mask: _____ . _____ . _____ . _____

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____ . _____ . _____ . _____

Secondary DNS Server IP Address: _____ . _____ . _____ . _____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

Connecting the Model RP614 v2 Web Safe Router

This section provides instructions for connecting the RP614 v2 router. Also, the *Model RP614 v2 Resource CD* included with your router contains an animated Installation Assistant to help you through this procedure.

Procedure: Connecting the Router

There are three steps to connecting your router:

1. Connect the router to your network
2. Log in to the router
3. Connect to the Internet

Follow the steps below to connect your router to your network. You can also refer to the Resource CD included with your router which contains an animated Installation Assistant to help you through this procedure.

1. Connect the router to your network.

    a. Turn off your computer and Cable or DSL Modem.

    b. Disconnect the Ethernet cable (A) from your computer which connects to your cable or DSL modem.
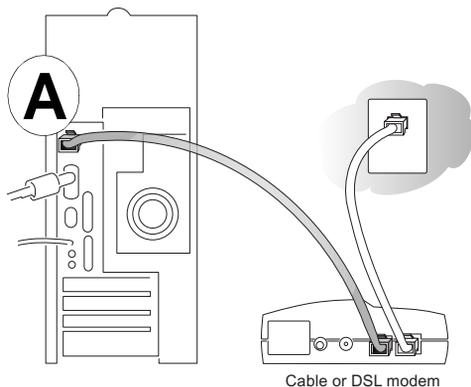
Cable or DSL modem

Figure 2-1: Disconnect the cable or DSL Modem

c. Connect the Ethernet cable from your cable or DSL modem to the Internet port (A) on the Model RP614 v2.
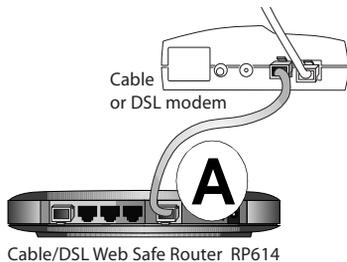
Figure 2-2: Connect the cable or DSL Modem to the router

d. Connect the Ethernet cable which came with the router from a Local port on the router (B) to your computer.
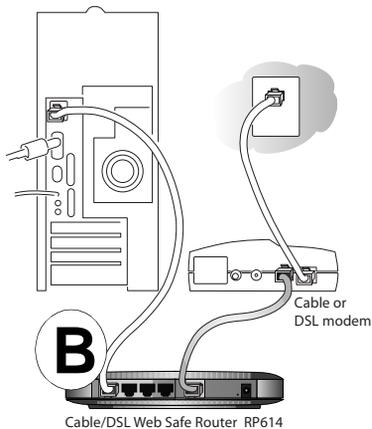
Figure 2-3: Connect the computers on your network to the router

Note: The RP614 v2 router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense if the cable should have a normal connection or an uplink connection. This feature eliminates the need to worry about crossover cables because Auto Uplink will make the right connection either type of cable.

e. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software or cancel it if it starts automatically.

f.   Verify the following:

When your turn the router on, the power light goes on.

The test light turns on within a few seconds, and then goes off after approximately 10 seconds.

The router's local lights are lit for any computers that are connected to it.

The router's Internet light is lit, indicating a link has been established to the cable or DSL modem.

2. Log in to the router.

Note: To connect to the router, your computer needs to be configured to obtain an IP address automatically via DHCP. If you need instructions on how to do this, please refer to Appendix C, "Preparing Your Network".

a.   Connect to the router by typing *http://192.168.0.1* in the address filed of Internet Explorer or Netscape® Navigator.
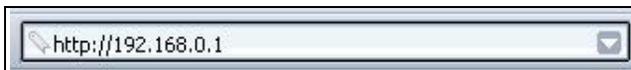
Figure 2-4: Log in to the router

b.   For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters.

Note: The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

A login window shown below opens:

Figure 2-5: Login window
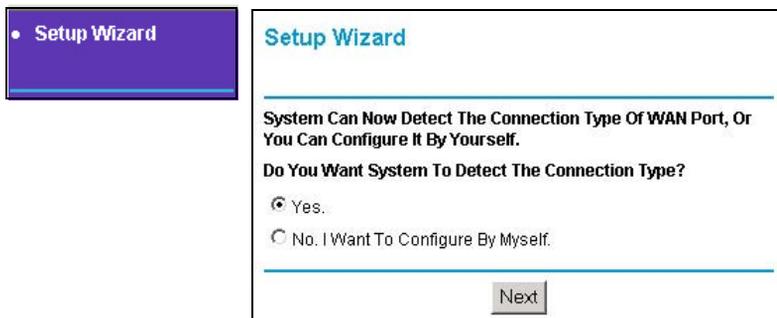
3.   Connect to the Internet

Figure 2-6: Setup Wizard

a.   You are now connected to the router. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu.

b.   Click Next and follow the steps in the Setup Wizard for inputting the configuration parameters from your ISP to connect to the Internet.

Note: If you choose not to use the Setup Wizard, you can manually configure your Internet connection settings by following the procedure "Manually Configuring Your Internet Connection" on page 2-16.

Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP as you recorded them previously in "Worksheet to Record Your Internet Connection Information" on page 2-3.

c. When the router successfully detects an active Internet service, the router's Internet LED goes on. The Setup Wizard reports which connection type it discovered, and displays the appropriate configuration menu. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your router and the cable or DSL line.

d. The Setup Wizard will report the type of connection it finds. The options are:

- Connections which require a login using protocols such as PPPoE, AOL, PPTP, Telstra, or Bigpond broadband connections.
- Connections which use dynamic IP address assignment.
- Connections which use fixed IP address assignment.

The procedures for filling in the configuration menu for each type of connection follow below.

PPPoE Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses PPPoE, you will see this menu:

Figure 2-7: Setup Wizard menu for PPPoE accounts

- Enter the Account Name, Domain Name, Login, and Password as provided by your ISP. These fields are case sensitive. The router will try to discover the domain automatically if you leave the Domain Name blank. Otherwise, you may need to enter it manually.

- To change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.

  Note: You no longer need to run the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your router will automatically log you in.

- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

  Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- Click Apply to save your settings.

- Click Test to verify that your Internet connection works. If the NETGEAR website does not appear within one minute, refer to Chapter 6, "Troubleshooting."

AOL Wizard-Detected Options

> **Note:** If you have an AOL account, any computer connected to the router must use the AOL software to connect to the Internet through the router. If you have not already done so, install the AOL software on your PC now. Be sure to install the AOL Home Network updates as well. AOL v8.0 software is included on the *Model RP614 v2 Resource CD* which came with your Model RP614 v2.

- If the Setup Wizard discovers that AOL is your ISP, you will see a screen like the one below:
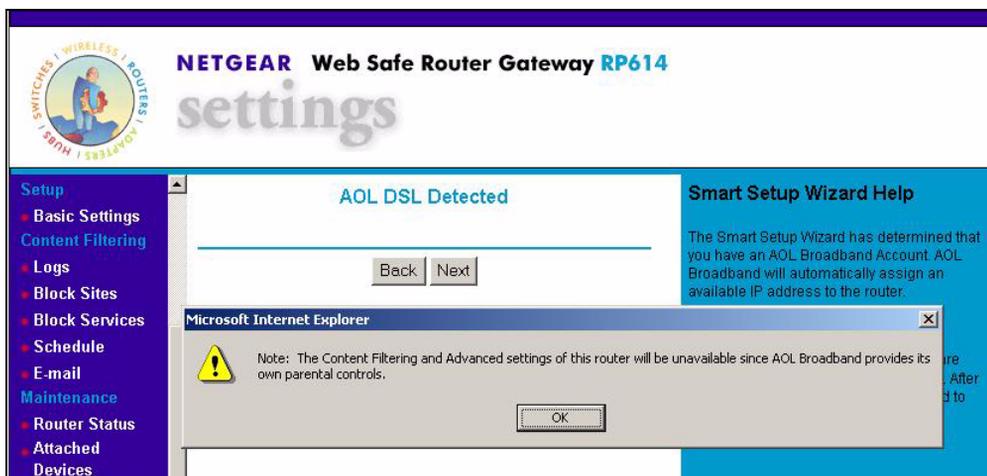
Figure 2-8: AOL detected

- When the Setup Wizard detects an AOL DSL or Cable service, the RP614 v2 router automatically pre-configures itself to work with the AOL service.

  Note: Services such as AOL which use L2TP tunneling will bypass the firewall feature included with your router. For additional home network security, install the PC-based Freedom Firewall software application included on your *Model RP614 v2 Resource CD*.

- Click OK to continue. The filtering features of the Model RP614 v2 Web Safe Router are now turned off. You will notice that the navigation menu now looks like the illustration below.
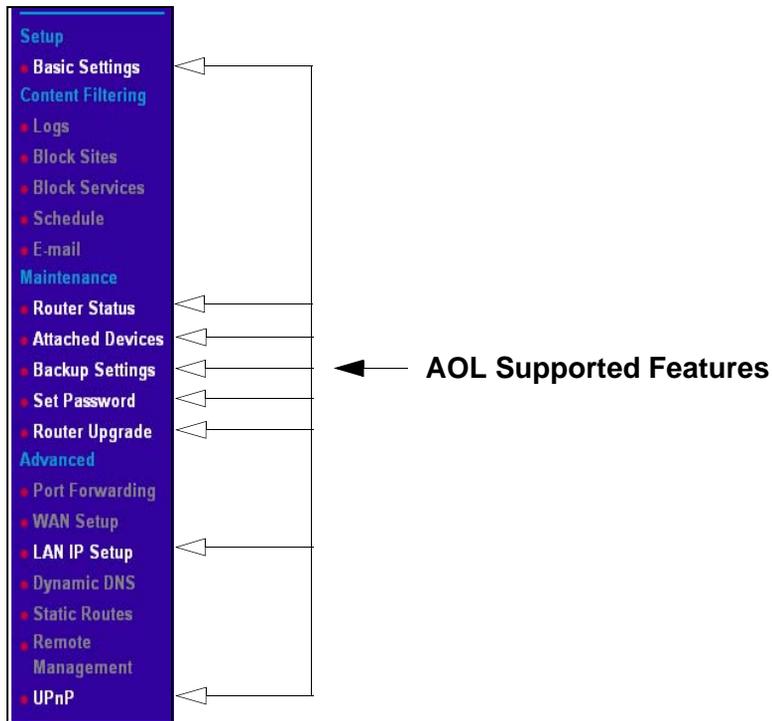
Figure 2-9: AOL supported features

• Next, the router synchronized with the AOL network and displays the message below.
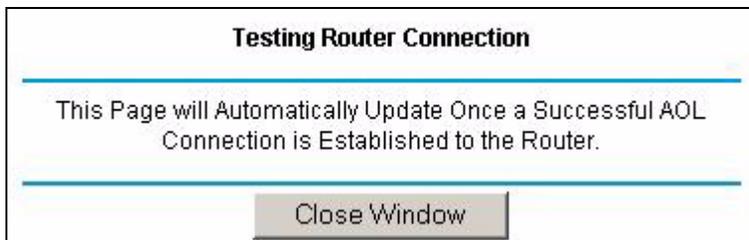
Figure 2-10: AOL network synchronization

• After the router finishes testing the connection, the window updates with the AOL Connection Established message below.
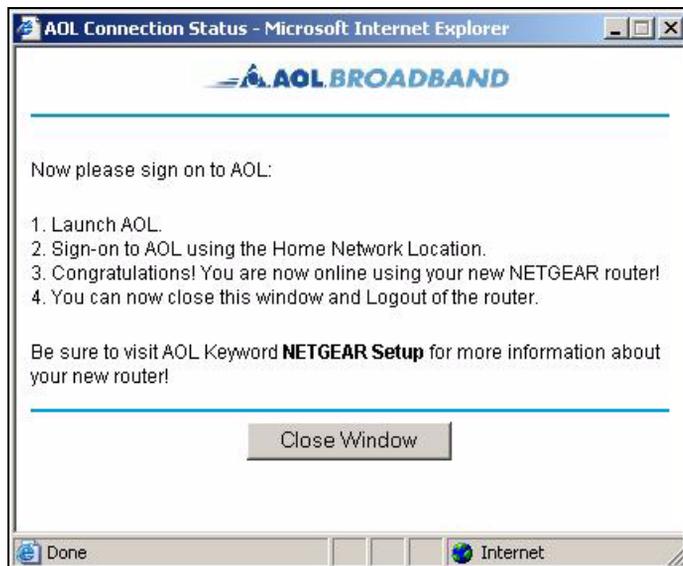
Figure 2-11: AOL connection established

• From a computer connected to the router, sign on to AOL as illustrated below.
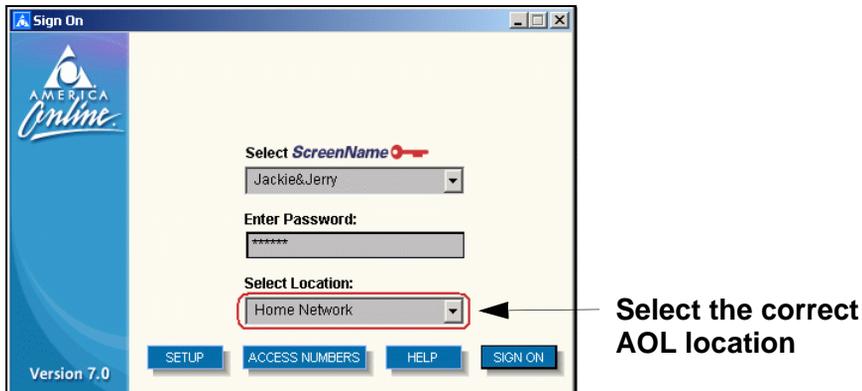
Figure 2-12: AOL sign on screen

Note: Be sure that the AOL Home Networking updates are installed, and be sure to select the correct AOL location: for AOL DSL, choose Home Networking; for AOL Cable, choose Home - Cable.

• This completes the configuration of the RP614 v2 router for connecting to your AOL account. Now, all the computers on your network can share the AOL Internet connection through the Model RP614 v2 Web Safe Router. To connect to the Internet, run the AOL software on a computer, select Home Network as the location, sign on, and the router will share the connection with others who are connected from different computers on the network.

Telstra Bigpond Cable Wizard-Detected Option

If the Setup Wizard discovers Telstra Bigpond Cable is your ISP, you will see this menu:

Figure 2-13: Setup Wizard menu for Telstra Bigpond Cable accounts

• Enter your Login, Password and Authentication Server. These fields are case sensitive.

  Note: You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your router will automatically log you in.

• The Domain Name Server (DNS) Address parameters may be necessary to access your ISP's services such as mail or news servers.
  Note: If you enter DNS addresses, restart your computers so that these settings take effect.

• Router MAC Address:
  This section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC.

  To change the MAC address, select "Use this Computer's MAC address." The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.

- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 6, "Troubleshooting.

Dynamic IP Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Dynamic IP assignment, you will see this menu:

Figure 2-14: Setup Wizard menu for Dynamic IP address accounts

- Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the router try to discover the domain. Otherwise, you may need to enter it manually.
- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use these DNS servers and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

  Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 6, "Troubleshooting."

Fixed IP Account Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Fixed IP assignment, you will see this menu:

Figure 2-15: Setup Wizard menu for Fixed IP address accounts

- Fixed IP is also called Static IP. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP. You will need the configuration parameters from your ISP you recorded in "Worksheet to Record Your Internet Connection Information" on page 2-3.
- Enter the IP address of your ISP's Primary and Secondary DNS Server addresses.

  Note: Restart the computers on your network so that these settings take effect.

- Click Apply to save the settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 6, "Troubleshooting."

Manually Configuring Your Internet Connection

You can manually configure your router using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

ISP *Does Not* Require Login   **ISP *Does* Require Login**
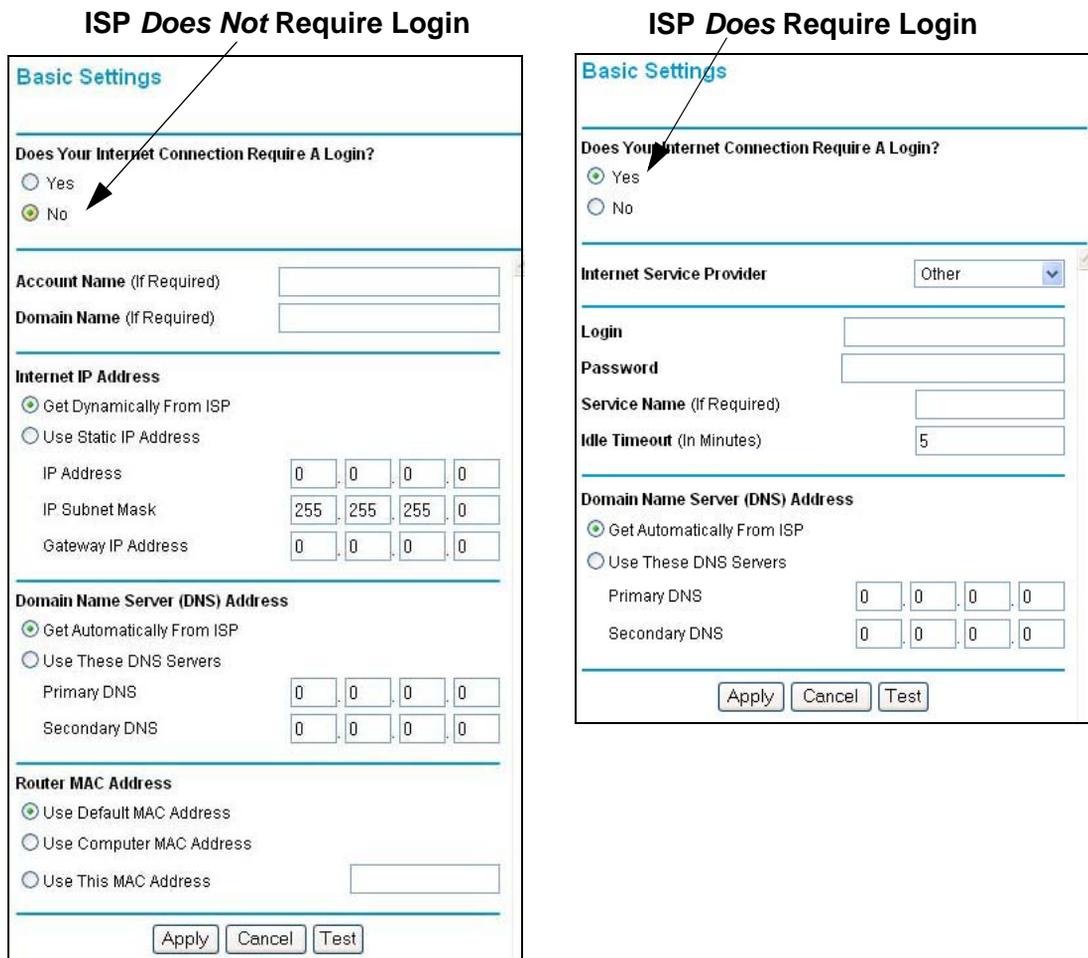
Figure 2-16: Browser-based configuration Basic Settings menus

Procedure: Configuring the Internet Connection Manually

You can manually configure the router using the Basic Settings menu shown in using these steps:

1. Click the Basic Settings link on the Setup menu.

2. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 3.

   a. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

   b. Internet IP Address:
      If your ISP has assigned you a permanent, fixed (static) IP address for your PC, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.

   c. Domain Name Server (DNS) Address:
      If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

      Note: If you enter an address here, restart the computers on your network so that these settings take effect.

   d. Gateway's MAC Address:
      This section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC by "cloning" its MAC address.

      To change the MAC address, select "Use this Computer's MAC address." The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.

   e. Click Apply to save your settings.

3. If your Internet connection does require a login, fill in the settings according to the instructions below. Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

Note: After you finish setting up your router, you will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your router will automatically log you in.

a. Select you Internet service provisory from the drop-down list.

Figure 2-17: Basic Settings ISP list

b. The screen will change according to the ISP settings requirements of the ISP you select.

c. Fill in the parameters for your ISP according to the Wizard-detected procedures starting on page 2-8.

d. Click Apply to save your settings.

Chapter 3
Content Filtering

This chapter describes how to use the content filtering features of the Model RP614 v2 Web Safe Router to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

Content Filtering Overview

The Model RP614 v2 Web Safe Router provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web addresses and web address keywords. You can also block Internet access by applications and services, such as chat or games.

To configure these features of your router, click on the subheadings under the Content Filtering heading in the Main Menu of the browser interface. The subheadings are described below:

Blocking Access to Internet Sites

The RP614 v2 router allows you to restrict access based on web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in Figure 3-1 below:
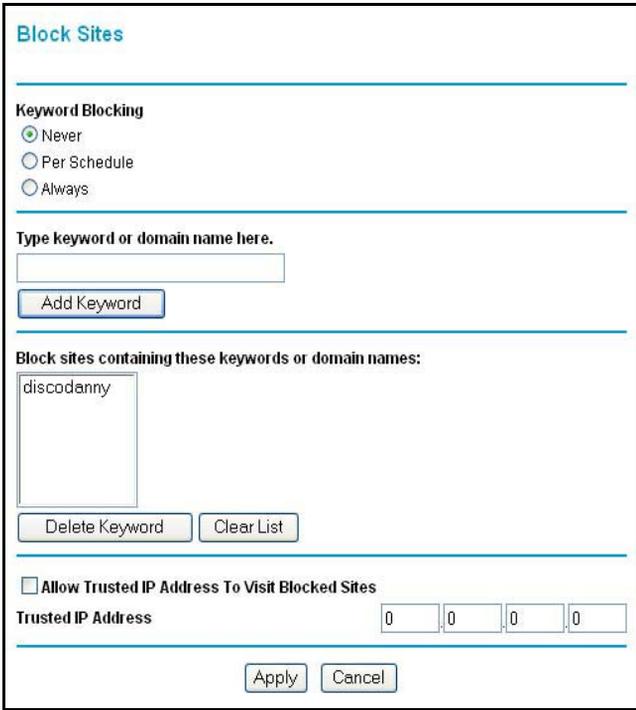
Block Sites

Keyword Blocking
- ⦿ Never
- ○ Per Schedule
- ○ Always

Type keyword or domain name here.

[   ]

[Add Keyword]

Block sites containing these keywords or domain names:

discodanny

[Delete Keyword]   [Clear List]

☐ **Allow Trusted IP Address To Visit Blocked Sites**

Trusted IP Address   [0] . [0] . [0] . [0]

[Apply] [Cancel]

Figure 3-1: Block Sites menu

To enable keyword blocking, select either "Per Schedule" or "Always", then click Apply. If you want to block by schedule, be sure that a time period is specified in the Schedule menu.

To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

Keyword application examples:

• If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.

- If the keyword ".com" is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.

- If you wish to block all Internet browsing access during a scheduled period, enter the keyword "." and set the schedule in the Schedule menu.

To specify a Trusted User, enter that PC's IP address in the Trusted User box and click Apply.

You may specify one Trusted User, which is a PC that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that PC with a fixed IP address.

Blocking Access to Internet Services

The RP614 v2 router allows you to block the use of certain Internet services by PCs on your network. This is called services blocking or port filtering. The Block Services menu is shown below:

Figure 3-2: Block Services menu

Services are functions performed by server computers at the request of client computers. For example, Web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To enable service blocking, select either Per Schedule or Always, then click Apply. If you want to block by schedule, be sure that a time period is specified in the Schedule menu.

To specify a service for blocking, click Add. The Add Services menu will appear, as shown below:

Block Services

Service Type	HTTP	
Protocol	TCP	
Starting Port	80	(1~65535)
Ending Port	80	(1~65535)
Service Type/User Defined	HTTP	

Filter IP by :

⦿ Only this IP: 192 . 168 . 0 .

○ IP address range: 192 . 168 . 0 .
     to 192 . 168 . 0 .

○ Every IP

OK   Cancel

Figure 3-3: Add Services menu

From the Service Type list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select User Defined.

Configuring a User Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups.

Enter the Starting Port and Ending Port numbers. If the application uses a single port number, enter that number in both boxes.

If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select Both.

Configuring Services Blocking by IP Address Range

Under "Filter Services For", you can block the specified service for a single PC, a range of PCs (having consecutive IP addresses), or all PCs on your network.

Scheduling When Blocking Will Be Enforced

The RP614 v2 router allows you to specify when blocking will be enforced. The Schedule menu is shown below:
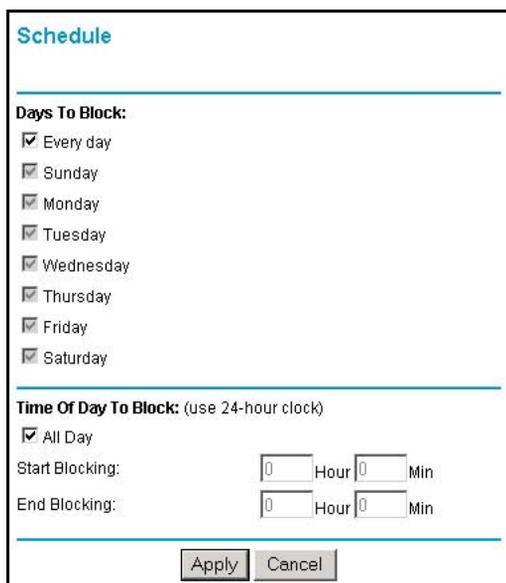
Schedule

Days To Block:
- ☑ Every day
- ☑ Sunday
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- ☑ Saturday

Time Of Day To Block: (use 24-hour clock)
- ☑ All Day

Start Blocking: [0] Hour [0] Min

End Blocking: [0] Hour [0] Min

[Apply] [Cancel]

Figure 3-4: Schedule menu

- Use this schedule for blocking content. Check this box if you wish to enable a schedule for Content Filtering. Click Apply.

- Days to Block. Select days to block by checking the appropriate boxes. Select Everyday to check the boxes for all days. Click Apply.

- Time of Day to Block. Select a start and end time in 23:59 format. Select All day for 24 hour blocking. Click Apply.

Be sure to select your Time Zone in the E-Mail menu.

Stateful Packet Inspection (SPI), Java, ActiveX, and Cookies Blocking Options

The WAN Setup options let you enable SPI and blocking of Java, ActiveX, and Cookies. These options are discussed below.

Using SPI

Stateful inspection technology tracks each packet traversing the router and makes sure that they are legitimate. A stateful inspection router also monitors the state of the connection and compiles the information in a state table ensuring that the source and destination of each packet is valid. By default, SPI is enabled.

You access the SPI and the Java, ActiveX, and Cookies blocking options from the WAN Setup menu, as shown below.

Figure 3-5: WAN Setup menu.

Using Java, ActiveX, and cookies Filtering.

What are these items and what can I do about them?

- ActiveX and Java programs can be embedded in websites, and will be executed by your computer. These programs may sometimes include malicious content.

- Cookies are small files that a website can store on your computer to track your activity. Some cookies can be helpful, but some may compromise your privacy.

To block these items, follow these steps:

1. Click WAN Setup link on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.

3. To block ActiveX, Java, Cookies, or Web Proxy functions for all Internet sites, click the check box next to the function and then click Apply.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of what websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries will only appear when keyword blocking is enabled, and no log entries will be made for the Trusted User. An example is shown below:
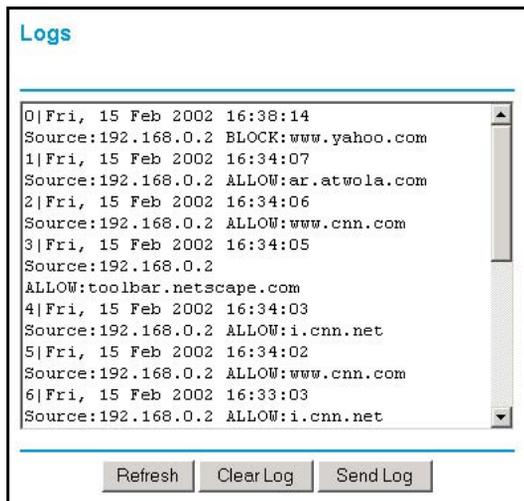
Figure 3-6: Logs menu

Log entries are described in Table 3-1

Table 3-1.   Log entry descriptions

Field	Description
Number	The index number of the content filter log entries. 128 entries are available numbered from 0 to 127. The log will keep the record of the latest 128 entries.
Date and Time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Action	This field displays whether the access was blocked or allowed.
	The name or IP address of the website or newsgroup visited or attempted to access.

Log action buttons are described in Table 3-2

Table 3-2.   Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.

Configuring E-Mail Alert and Web Access Log Notifications

In order to receive logs and alerts by email, you must provide your email information in the E-Mail menu, shown below:

Figure 3-7: Email menu

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the router.

- Your outgoing mail server
  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

- Send to this e-mail address
  Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately
  Check this box if you would like immediate notification of attempted access to a blocked site.

- Send logs according to this schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

  – Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.

  – Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

The RP614 v2 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone
  Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.

- Daylight Savings Time
  Check this box if your time zone is currently under daylight savings time.

This chapter describes how to use the maintenance features of your Model RP614 v2 Web Safe Router. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Viewing Router Status Information

The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, click on Maintenance, then select System Status to view the System Status screen, shown below.

Router Status

Account Name	
Firmware Version	1.00 RC11 Jan 29 2003
Internet Port	
MAC Address	00:09:5B:3B:1B:59
IP Address	10.1.0.161
DHCP	Client
IP Subnet Mask	255.255.254.0
Domain Name Server	10.1.1.6
	10.1.1.7
LAN Port	
MAC Address	00:09:5B:3B:1B:58
IP Address	192.168.0.1
DHCP	Server
IP Subnet Mask	255.255.255.0

Figure 4-1.   Router Status screen

This screen shows the following parameters:

Table 4-1.   Menu 3.2 - Router Status Fields

Field	Description
Account Name	This field displays the Host Name assigned to the router.
Firmware Version	This field displays the router firmware version.
Internet Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the Media Access Control address being used by the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the router.
MAC Address	This field displays the Media Access Control address being used by the LAN port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.

Click on the "Connection Status" button to display the connection status, as shown below.

Connection Status

IP Address	10.1.1.98
Subnet Mask	255.255.255.0
Default Gateway	10.1.1.13
DHCP Server	10.1.1.7
DNS Server	10.1.1.6
Lease Obtained	20:06:50 , Wednesday.
Lease Expires	21:06:50 , Wednesday.

[Release] [Renew]

[Close Window]

Figure 4-2.   Connection Status screen

This screen shows the following statistics:.

Table 4-1.   Connection Status Fields

Field	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DHCP Server	The WAN (Internet) DHCP Server the router communicates with.
DNS Server	The WAN (Internet) DNS Server for the router.
Lease Obtained	When the DHCP lease started.
Lease Expires	When the DHCP lease will expire.

Log action buttons are described in Table 4-2

Table 4-2.   Connection Status action buttons

Field	Description
Release	Click the Release button to release the DHCP lease.
Renew	Click the Renew button to renew the DHCP lease.
Close Window	Click this button to close the window.

Click on the "Show Statistics" button to display router usage statistics, as shown below.

Figure 4-3.   Router Statistics screen

This screen shows the following statistics:.

Table 4-1.   Router Statistics Fields

Field	Description
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.

Table 4-1. Router Statistics Fields (continued)

Field	Description
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown below.
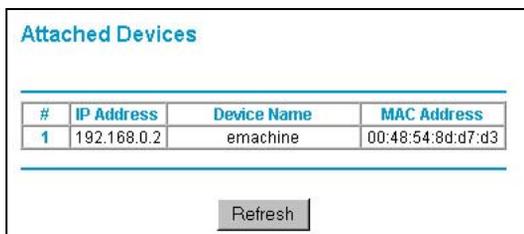
Figure 4-4. Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

Upgrading the Router Software

The routing software of the RP614 v2 router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file before sending it to the router. The upgrade file can be sent to the router using your browser.

Note: The Web browser used to upload new firmware into the RP614 v2 router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0 or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown below.
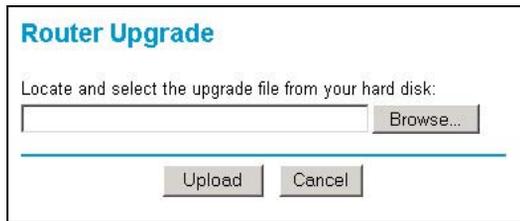
Router Upgrade

Locate and select the upgrade file from your hard disk:

[   ] Browse...

Upload   Cancel

Figure 4-5.   Router Upgrade menu

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.

2. In the Router Upgrade menu, click the Browse button and browse to the location of the binary (.BIN) upgrade file

3. Click Upload.

    Note: When uploading software to the RP614 v2 router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process will typically take about one minute.

In some cases, you may need to reconfigure the router after upgrading.

Configuration File Management

The configuration settings of the RP614 v2 router are stored within the router in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

From the Main Menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown below.
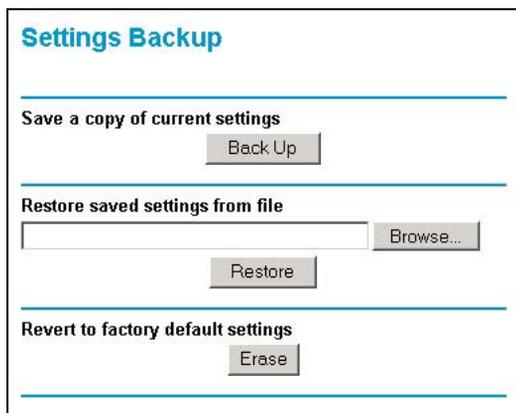
Figure 4-6.   Settings Backup menu

Three options are available, and are described in the following sections.

Restoring and Backing Up the Configuration

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your router's configuration settings.

To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file from the router and will prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the Browse button to browse to the file. When you have located it, click the Restore button to send the file to the router. The router will then reboot automatically.

Erasing the Configuration

It is sometimes desirable to restore the router to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

To erase the configuration, click the Erase button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Restoring the Default Configuration and Password" on page 6-7.

Changing the Configuration Password

The default password for the router's Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password.

From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown below.
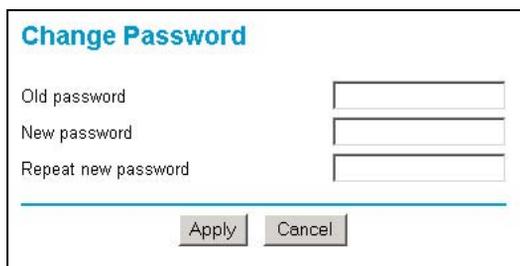
Change Password

Old password	
New password	
Repeat new password	

Apply   Cancel

Figure 4-7.   Set Password menu

To change the password, first enter the old password, and then enter the new password twice. Click Apply.

Chapter 5
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your Model RP614 v2 Web Safe Router. These features can be found under the Advanced heading in the Main Menu of the browser interface.

Configuring for Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Main Menu of the browser interface, under Advanced, click on Port Forwarding to view the port forwarding menu, shown below.

Figure 5-1: Port Forwarding Menu

> **Note:** If you are unfamiliar with networking and routing, refer to Appendix B, "Networks, Routing, and Firewall Basics," to become more familiar with the terms and procedures used in this manual.

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the Security Menu.

Before starting, you'll need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. Be sure the computer's IP address never changes. To configure port forwarding to a local server:

1. From the Service & Game box, select the service or game that you will host on your network. If the service does not appear in the list, refer to the following section, "Adding a Custom Service".

2. Enter the IP address of the local server in the corresponding Server IP Address box.

3. Click the Add button.

Adding a Custom Service

To define a service, game or application that does not appear in the Services & Games list, you must determine what port numbers are used by the service. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Click the Add Custom Service button.

2. Enter the first port number in an unused Start Port box.

3. To forward only one port, enter it again in the End Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.

4. Enter the IP address of the local server in the corresponding Server IP Address box.

5. Type a name for the service.

6. Click Apply at the bottom of the menu.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry, follow these steps.

1. In the table, select the button next to the service name.

2. Click Edit or Delete.

Local Web and FTP Server Example

If a local PC with a private IP address of 192.168.0.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.0.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account's IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.

- If the IP address of the local PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, you can manually configure the PC to use a fixed address.

- Local PCs must access the local server using the PCs' local LAN address (192.168.0.33 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

Multiple Computers for Half Life, KALI or Quake III Example

To set up an additional computer to play Half Life, KALI or Quake III:

1. Click the button of an unused port in the table.

2. Select the game again from the Services/Games list.

3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you've already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.

4. Type the same port number in the End Port box that you typed in the Start Port box.

5. Type the IP address of the additional computer in the Server IP Address box.

6. Click Apply.

Some online games and videoconferencing applications are incompatible with NAT. The RP614 v2 router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the default in the PORTS Menu. If one local PC acts as a game or videoconferencing host, enter its IP address as the default.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ server, change the MTU size and enable the router to respond to a Ping on the WAN port. These options are discussed below.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the default DMZ server.

> **Note:** DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu, shown below lets you configure a Default DMZ Server.

Figure 5-2: WAN Setup menu.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click WAN Setup link on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
3. Click Apply.

Respond to Ping on Internet WAN Port

If you want the router to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Don't check this box unless you have a specific reason to do so.

Setting the MTU Size

The default MTU size is usually fine. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU. This should not be done unless you are sure it is necessary by your ISP.

Any packets sent through the router that are larger than the configured MTU size will be repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

1. Under MTU Size, enter a new size between 64 and 1500.

2. Click Apply to save the new configuration.

Using the LAN IP Setup Options

The second feature category under the Advanced heading is LAN IP Setup. This menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown below.

Figure 5-3: LAN IP Setup Menu

Configuring LAN TCP/IP Setup Parameters

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act.as a DHCP server. The router's default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the router.

- IP Subnet Mask
  This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.

  — When set to Both or Out Only, the router will broadcast its routing table periodically.

  — When set to Both or In Only, it will incorporate the RIP information that it receives.

  — When set to None, it will not send any RIP packets and will ignore any RIP packets received.

- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.

  — RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.

  — RIP-2 carries more information. RIP-2B uses subnet broadcasting.

→ **Note:** If you change the LAN IP address of the router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

Using the Router as a DHCP server

By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "IP Configuration by DHCP" on page B-11 for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the 'Use router as DHCP server' check box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The router will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the router's LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router's LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it access the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the Add button.

2. In the IP Address box, type the IP address to assign to the PC or server.
    (choose an IP address from the router's LAN subnet, such as 192.168.0.X)

3. Type the MAC Address of the PC or server.
    (Tip: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)

4. Click Apply to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the PC contacts the router's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.

2. Click Edit or Delete.

Using a Dynamic DNS Service

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, who will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently-changing IP address.

> **Note:** If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the dynamic DNS service will not work because private addresses will not be routed on the Internet.

The router contains a client that can connect to many popular dynamic DNS services. You can select one of these services and obtain an account with them. Then, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS. To configure Dynamic DNS:

1. Register for an account with one of the dynamic DNS service providers whose names appear in the 'Select Service Provider' box. For example, for dyndns.org, go to www.dyndns.org.

2. Select the Use a dynamic DNS service check box.

3. Select the name of your dynamic DNS Service Provider.

4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.

5. Type the User Name for your dynamic DNS account.

6. Type the Password (or key) for your dynamic DNS account.

7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org

8. Click Apply to save your configuration.

Configuring Static Routes

Static Routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Route menu, shown below.

Figure 5-4.   Static Route Summary Table

To add or edit a Static Route:

1.   Click the Add button to open the Add/Edit Menu, shown below.

Figure 5-5.   Static Route Entry and Edit Menu

2.   Type a route name for this static route in the Route Name box under the table.
     (This is for identification purpose only.)

3.   Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.

4.   Select Active to make this route effective.

5.   Type the Destination IP Address of the final destination.

6. Type the IP Subnet Mask for this destination.
    If the destination is a single host, type 255.255.255.255.

7. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.

8. Type a number between 1 and 15 as the Metric value.
    This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

9. Click Apply to have the static route entered into the table.

As an example of when a static route is needed, consider the following case:

-   Your primary Internet access is through a cable modem to an ISP.

-   You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.

-   Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like .

In this example:

-   The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.

-   The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.

-   A Metric value of 1 will work since the ISDN router is on the LAN.

-   Private is selected only as a precautionary security measure in case RIP is activated.

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your RP614 v2 router.

> **Note:** Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for Remote Management:

1. Select the Turn Remote Management On check box.

2. Specify what external addresses will be allowed to access the router's remote management.

   Note: For enhanced security, restrict access to as few external IP addresses as practical.

   a. To allow access from any IP address on the Internet, select Everyone.

   b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

   c. To allow access from a single IP address on the Internet, select Only this PC. Enter the IP address that will be allowed access.

3. Specify the Port Number that will be used for accessing the management interface.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click Apply to have your changes take effect.

Note: When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, you must enter in your browser:

```
http://134.177.0.123:8080
```

Using Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) [30]

Advertisement Time To Live (in hops) [0]

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

[Apply] [Cancel] [Refresh]

Figure 5-6.   UPnP Menu

From the Main Menu of the browser interface, under Advanced, click on UPnP. Set up UPnP according to the guidelines below.

Turn UPnP On: UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

Advertisement Period: The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

Advertisement Time To Live: The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.

UPnP Portmap Table: The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

Advanced Configuration of the Router

Chapter 6
Troubleshooting

This chapter gives information about troubleshooting your Model RP614 v2 Web Safe Router. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Operation

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED ⏻ is on.

2. Verify that the Test LED ✓ lights within a few seconds, indicating that the self-test procedure is running.

3. After approximately 10 seconds, verify that:

   a. The Test LED is not lit.

   b. The LAN port LEDs are lit for any local ports that are connected.

   c. The WAN port LED is lit.

   If a port's LED is lit, a link has been established to the connected device. If an Ethernet port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.

- Check that you are using the 7.5 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

Test LED Never Turns On or Test LED Stays On

When the router is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the router.

If you experience problems with the Test LED:

- Cycle the power to see if the router recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the router recovers.

- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 6-7.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.

- Make sure that power is turned on to the connected hub or workstation.

- Be sure you are using the correct cable:

  — When connecting the router's WAN port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the router as described in the previous section.

- Make sure your PC's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Verifying TCP/IP Properties" on page 4-5 or "Verifying TCP/IP Properties (Macintosh)" on page 4-8 to find your PC's IP address. Follow the instructions in Chapter 4 to configure your PC.

   Note: If your PC's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the router and reboot your PC.

- If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 6-7.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.

- Try quitting the browser and launching it again.

- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.

- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com

2. Access the Main Menu of the router's configuration at http://192.168.0.1

3. Under the Maintenance heading, select Router Status

4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new router by performing the following procedure:

1. Turn off power to the cable or DSL modem.

2. Turn off power to your router.

3. Wait five minutes and reapply power to the cable or DSL modem.

4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your router.

If your router is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, you may have incorrectly set the login name and password.

- Your ISP may check for your PC's host name.
  Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.

- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

OR

Configure your router to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring Your Internet Connection" on page 2-16.

If your router can obtain an IP address, but your PC is unable to load any web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your PC and verify the DNS address as described in "Verifying TCP/IP Properties" on page 4-5. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC may not have the router configured as its TCP/IP gateway.

  If your PC obtains its information from the router by DHCP, reboot the PC and verify the gateway address as described in "Verifying TCP/IP Properties" on page 4-5.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your PC or workstation.

Testing the LAN Path to Your Router

You can ping the router from your PC to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.

2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   ping 192.168.0.1

3. Click on OK.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

If the path is not working, you see this message:

Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On" on page 6-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

PING -n 10 *<IP address>*

where *<IP address>* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in "Verifying TCP/IP Properties" on page 4-5.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring Your Internet Connection" on page 2-16.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

• Use the Erase function of the router (see "Erasing the Configuration" on page 4-8).

• Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).

2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The RP614 v2 router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

• Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.

• Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

Appendix A
Technical Specifications

This appendix provides technical specifications for the Model RP614 v2 Web Safe Router.

Specifications for the Model RP614 v2

The table below lists the technical specifications for the Model RP614 v2.

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPTP, Telstra BigPond, PPP over Ethernet (PPPoE)

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	7.5 V DC @ 1A output, 20W maximum

Physical Specifications

Dimensions:	28 x 175 x 118 mm (1.1 x 6.89 x 4.65 in.)
Weight:	0.3 kg (0.66 lb)
Environmental Specifications	
Operating temperature:	32°-140° F (0° to 40° C)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
Local:	10BASE-T or 100BASE-Tx, RJ-45
Internet:	10BASE-T, RJ-45

Appendix B
Networks, Routing, and Firewall Basics

This appendix provides an overview of IP networks, routing, and firewalls.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the <u>Internet Engineering Task Force</u> (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a <u>local area network</u> (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed <u>wide-area network</u> (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The RP614 v2 router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011   00100010   00001100   00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

Class A

Network   Node

Class B

            Network   Node

Class C
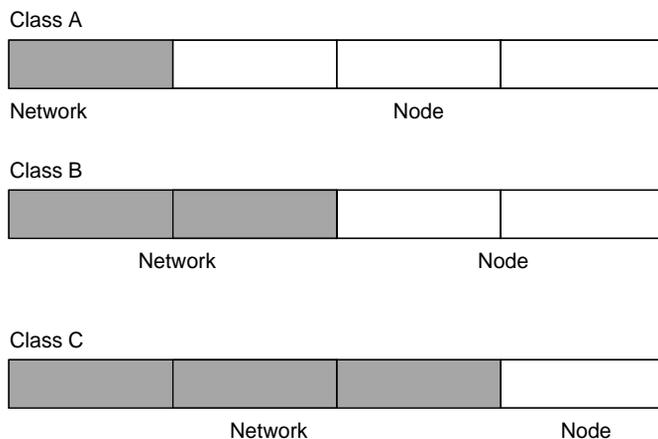
            Network   Node

Figure 6-1: Three Main Address Classes

The five address classes are:

* Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  1.x.x.x to 126.x.x.x.

* Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  128.1.x.x to 191.254.x.x.

- Class C

  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  192.0.1.x to 223.255.254.x.

- Class D

  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  224.0.0.0 to 239.255.255.255.

- Class E

  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000   10101000   10101010   11101101 (192.168.170.237)
```

combined with:

```
11111111   11111111   11111111   00000000 (255.255.255.0)
```

Equals:

```
11000000   10101000   10101010   00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as "/n." In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

Class B

| Network | Subnet | Node |

Figure 6-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

> **Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 6-1.   **Netmask Notation Translation Table for One Octet**

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 6-2.   **Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

• So that hosts recognize local IP broadcast packets.

When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

• So that a local router or bridge recognizes which addresses are local and which are remote.

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the RP614 v2 router is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space.* The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at *www.ietf.org*.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The RP614 v2 router employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

The following figure illustrates a single IP address operation.
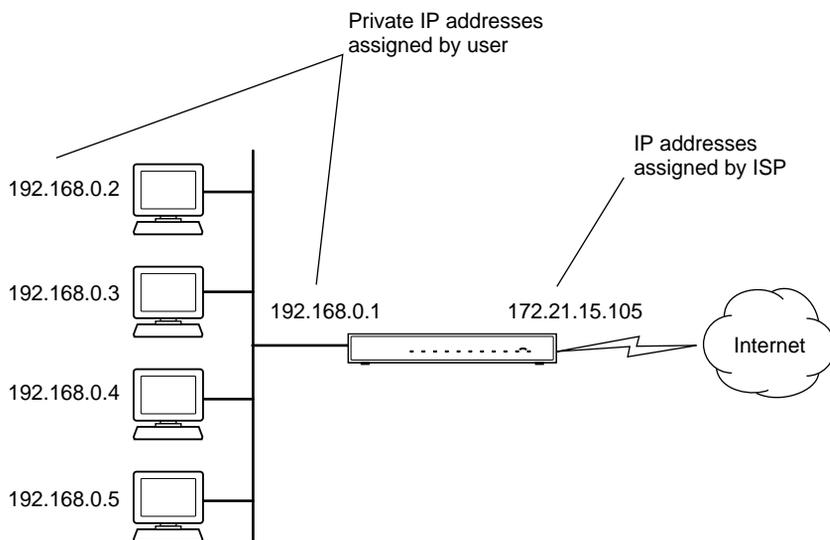
Figure 6-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are *not* available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a <u>Dynamic Host Configuration Protocol</u> (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The RP614 v2 router has the capacity to act as a DHCP server.

The RP614 v2 router also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the <u>Network Address Translation</u> (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send e-mail to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called <u>stateful packet inspection</u> to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using stateful packet inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or be rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use <u>unshielded twisted pair</u> (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described in Table 6-1.

Table 6-1.   UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as <u>Media Dependant Interface</u> (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as <u>Media Dependant Interface - Crossover</u> (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The RP614 v2 router incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (100BASE-TX) the cable must be rated as Category 5, (Cat 5), by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

This appendix describes how to prepare your network to connect to the Internet through the Model RP614 v2 Web Safe Router and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

> **Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-19 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-20 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.

- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.

- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

• All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network, Routing, Firewall, and Basics.""

The RP614 v2 router is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

• PC or workstation IP addresses—192.168.0.2 through 192.168.0.254

• Subnet mask—255.255.255.0

• Gateway address (the firewall)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:
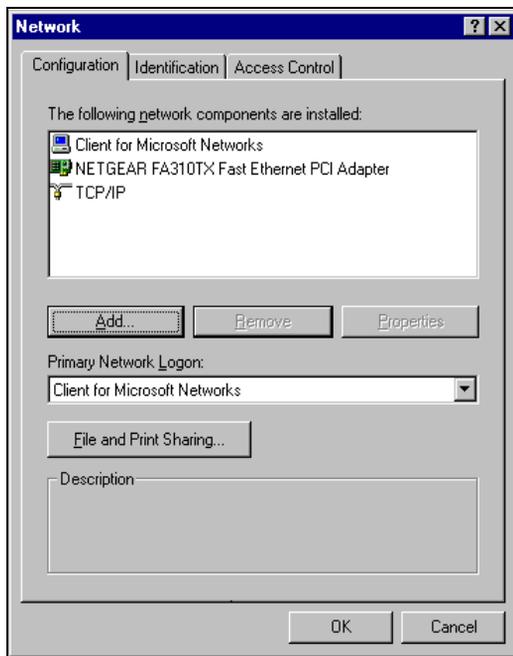
You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

→ **Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a.   Click the Add button.

b.   Select Client, and then click Add.

c.   Select Microsoft.

d.   Select Client for Microsoft Networks, and then click OK.

3.   Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

Locate your **Network Neighborhood** icon.

•   If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.

•   If the icon is not on the desktop,

   –   Click **Start** on the task bar located at the bottom left of the window.

   –   Choose **Settings**, and then **Control Panel**.

   –   Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

- Verify the following settings as shown:

    – Client for Microsoft Network exists

    – Ethernet adapter is present

    – TCP/IP is present

    – **Primary Network Logon** is set to Windows logon

- Click on the **Properties** button. The following TCP/IP Properties window will display.

Network ? ✕

Configuration | Identification | Access Control |

The following network components are installed:

🖳 Client for Microsoft Networks
🖧 3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
📡 TCP/IP

Add... | Remove | Properties

Primary Network Logon:

Client for Microsoft Networks ▼

Client for Microsoft Networks
Windows Logon

Description
The primary network logon is the client that is used to validate your user name and password, process any login scripts, and perform other startup tasks.

OK | Cancel

• By default, the **IP Address** tab is open on this window.

• Verify the following:

Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.

• Click **OK** to continue.

• Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.
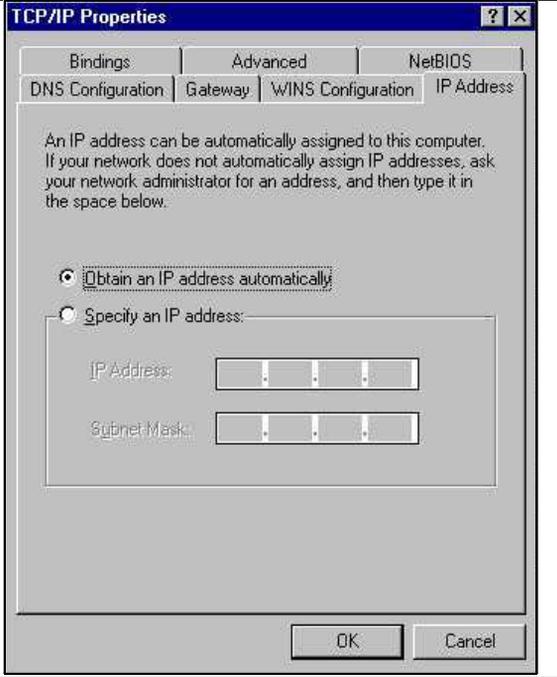
Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Internet Options icon.

3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.

4. Select "I want to connect through a Local Area Network" and click Next.

5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.

6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

    The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

    The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

    •   The IP address is between 192.168.0.2 and 192.168.0.254

    •   The subnet mask is 255.255.255.0

    •   The default gateway is 192.168.0.1

Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure
TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network and Dialup Connections icon.

3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.

4. Select Properties.

5. Verify that 'Client for Microsoft Networks' and 'Internet Protocol (TCP/IP)' are present. If not, select Install and add them.

6. Select 'Internet Protocol (TCP/IP)', click Properties, and verify that "Obtain an IP address automatically is selected.

7. Click OK and close all Network and Dialup Connections windows.

8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

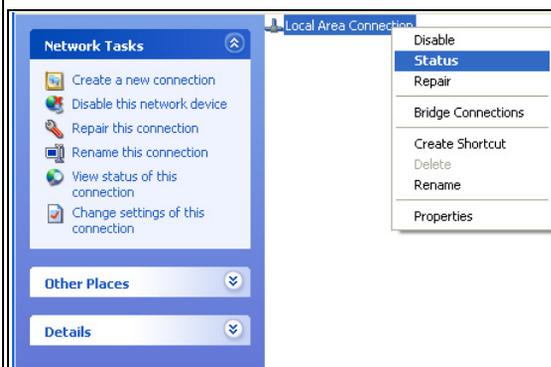Open your **Network Connections** window.

- Select **Network** from the Windows XP new Start Menu.

- Click the **Network Connections** link on the Network Tasks list.

2

- Now the Network Connection window displays.

  The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection** you will use and choose **Status**.

3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.

  Administrator logon access rights are needed to use this window.

- Click the **Properties** button to view details about the connection.
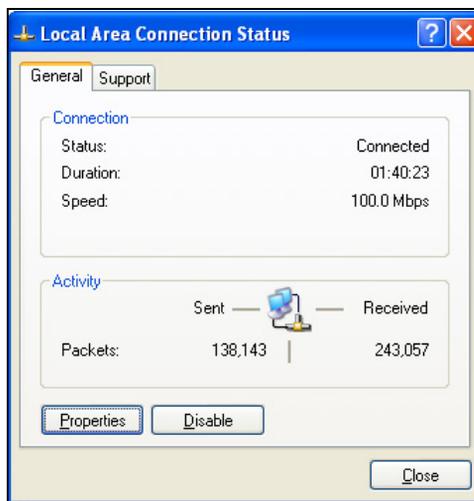
4

- The TCP/IP details are presented on the Support tab page.

- Select **Internet Protocol,** and click the **Properties** button to view the configuration information**.**

5

- Verify that the **Obtain an IP address automatically** radio button is selected.

- Verify that **Obtain DNS server address automatically** radio button is selected.
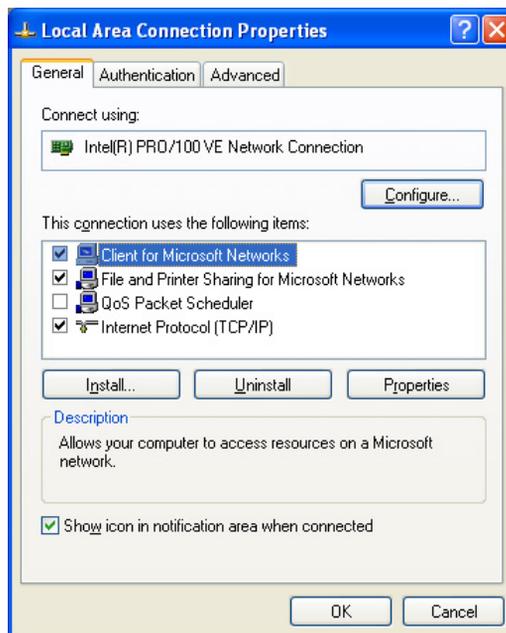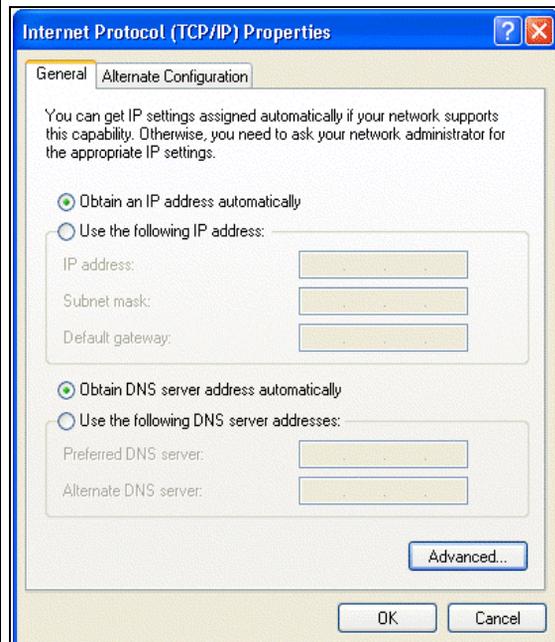
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ⊙ Obtain an IP address automatically
- ○ Use the following IP address:

    IP address:

    Subnet mask:

    Default gateway:

- ⊙ Obtain DNS server address automatically
- ○ Use the following DNS server addresses:

    Preferred DNS server:

    Alternate DNS server:

Advanced...

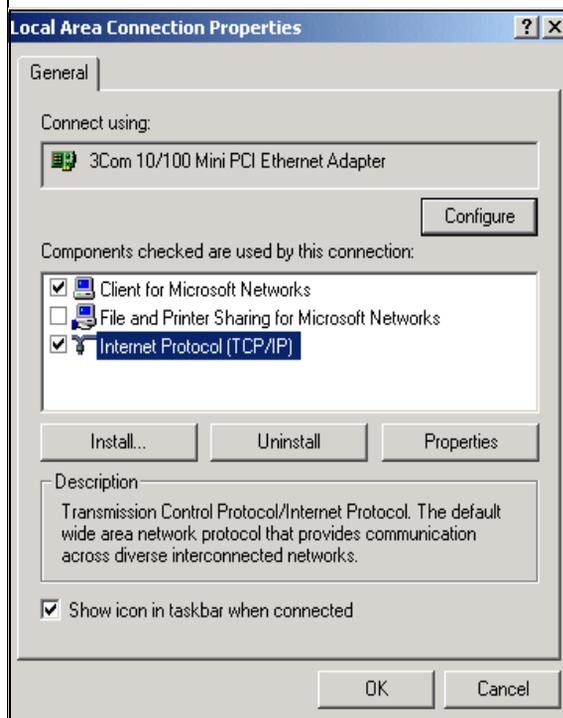OK   Cancel

DHCP Configuration of TCP/IP in Windows 2000

Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.

- Right click on **Local Area Connection** and select **Properties**.

2

- The **Local Area Connection Properties** dialog box appears.

- Verify that you have the correct Ethernet card selected in the **Connect using:** box.

- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"

  – Client for Microsoft Networks and

  – Internet Protocol (TCP/IP).

Local Area Connection Properties ? ×

General

Connect using:

🖧 3Com 10/100 Mini PCI Ethernet Adapter

Configure

Components checked are used by this connection:

☑ 🖳 Client for Microsoft Networks
☐ 🖳 File and Printer Sharing for Microsoft Networks
☑ 🍸 Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

OK | Cancel

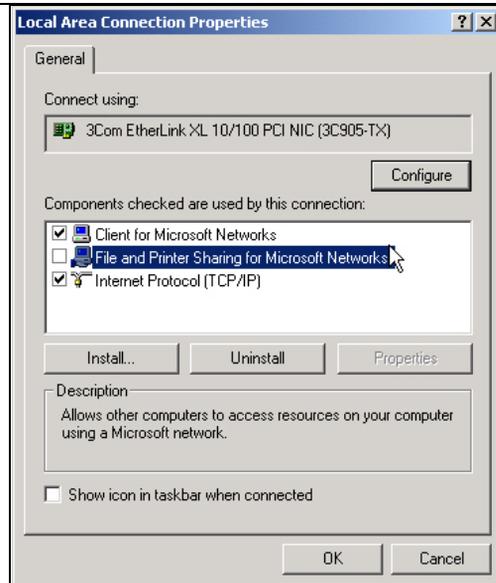|	
3	**Internet Protocol (TCP/IP) Properties** ? ✕ General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ◉ Obtain an IP address automatically ○ Use the following IP address: IP address: Subnet mask: Default gateway: ◉ Obtain DNS server address automatically ○ Use the following DNS server addresses: Preferred DNS server: Alternate DNS server: Advanced... OK Cancel

-
- With Internet Protocol (TCP/IP) selected, click on **Properties** button to open the Internet Protocol (TCP/IP) Properties dialogue box.

- Verify that

  – **Obtain an IP address automatically** is selected.

  – **Obtain DNS server address automatically** is selected.

- Click **OK** to return to Local Area Connection Properties.
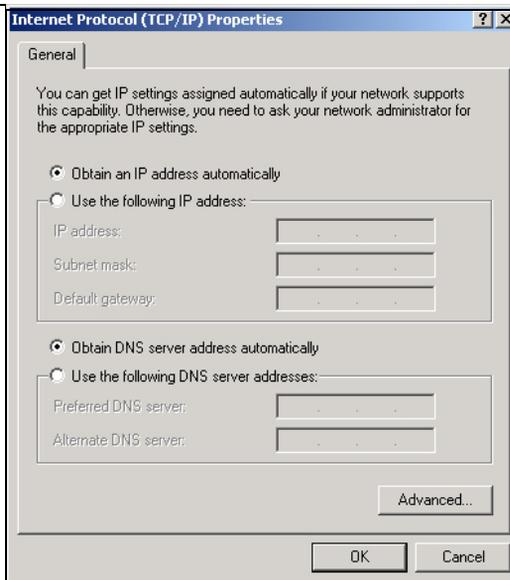
4

- Click **OK** again to complete the configuration process for Windows 2000.

- Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.

Local Area Connection Properties ? ✕

General

Connect using:

🖳 3Com EtherLink XL 10/100 PCI NIC (3C905-TX)

Configure

Components checked are used by this connection:

☑ 🖳 Client for Microsoft Networks
☐ 🖳 File and Printer Sharing for Microsoft Networks
☑ 🖳 Internet Protocol (TCP/IP)

Install...   Uninstall   Properties

Description
Allows other computers to access resources on your computer using a Microsoft network.

☐ Show icon in taskbar when connected

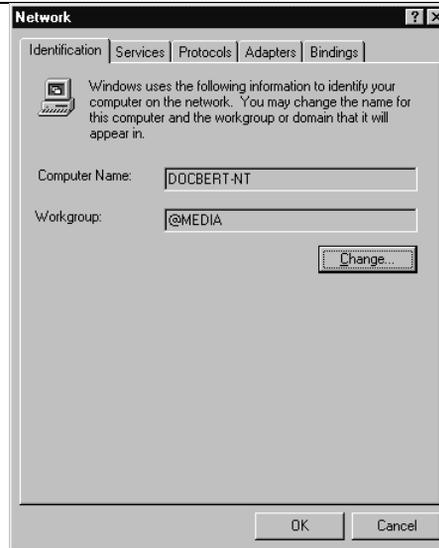OK   Cancel

DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

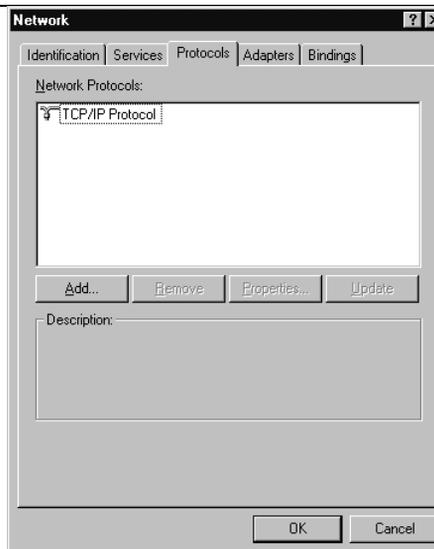• Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

2

• Double-click the **Network** icon in the Control Panel window.

  The Network panel will display.

• Select the **Protocols** tab to continue.

Network

Identification | Services | Protocols | Adapters | Bindings

Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: DOCBERT-NT

Workgroup: @MEDIA

Change...

OK | Cancel

3 • Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.	**Network** `? X` Identification | Services | Protocols | Adapters | Bindings | Network Protocols: TCP/IP Protocol Add... Remove Properties... Update Description: OK Cancel
4 • The **TCP/IP Properties** dialog box now displays. • Click the **IP Address** tab**.** • Select the radio button marked **Obtain an IP address from a DHCP server.** • Click **OK**. This completes the configuration of TCP/IP in Windows NT. • Restart the PC. Repeat these steps for each PC with this version of Windows on your network.	**Microsoft TCP/IP Properties** `? X` IP Address | DNS | WINS Address | Routing | An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below. Adapter: [1] 3Com Etherlink III PCI Bus-Master Adapter (3C590) ⦿ Obtain an IP address from a DHCP server ○ Specify an IP address IP Address: Subnet Mask: Default Gateway: Advanced... OK Cancel Apply

Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type `cmd` and then click OK.

   A command window opens

3. Type `ipconfig /all`

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   • The IP address is between 192.168.0.2 and 192.168.0.254

   • The subnet mask is 255.255.255.0

   • The default gateway is 192.168.0.1

4. Type `exit`

Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens:
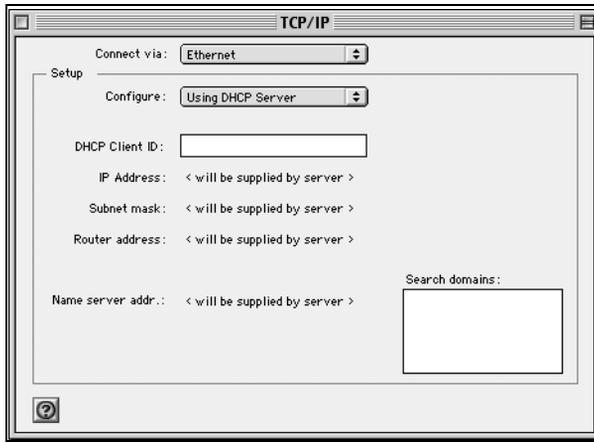
2. From the "Connect via" box, select your Macintosh's Ethernet interface.

3. From the "Configure" box, select Using DHCP Server.

    You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.

5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.

3. If not already selected, Select Using DHCP in the TCP/IP tab.

4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.
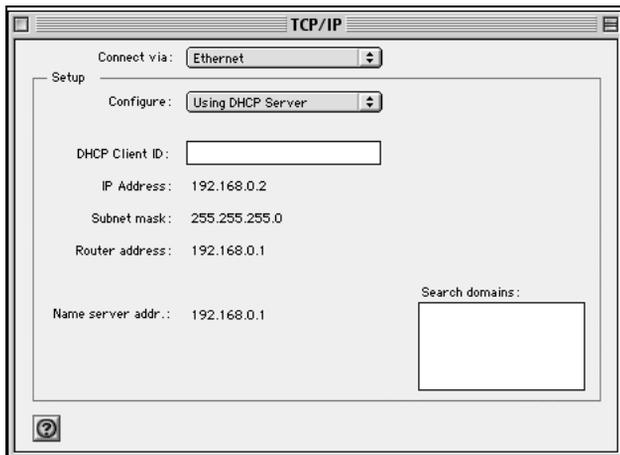
The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254

- The Subnet mask is 255.255.255.0

- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the "Configure" setting to a different option, then back again to "Using DHCP Server".

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask

- A gateway IP address, which is the address of the ISP's router

- One or more domain name server (DNS) IP addresses

- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the RP614 v2 router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.

3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".

5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

    If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

    You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the RP614 v2 router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

    The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your RP614 v2 router, you are ready to access and configure the firewall.

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
100BASE-Tx	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
802.11b	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
Denial of Service attack	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
DHCP	*See* Dynamic Host Configuration Protocol.
DNS	*See* Domain Name Server.
domain name	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
Domain Name Server	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
Dynamic Host Configuration Protocol	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
Gateway	A local device, usually a router, that connects hosts on a local network to other networks.
IP	*See* Internet Protocol.

IP Address	A four-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
IPSec	Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.
ISP	Internet service provider.
Internet Protocol	The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
LAN	*See* local area network.
local area network	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
MAC address	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
Mbps	Megabits per second.
MSB	*See* Most Significant Bit or Most Significant Byte.
MTU	*See* Maximum Transmission Unit.
Maximum Transmission Unit	The size in bytes of the largest packet that can be sent or received.
Most Significant Bit or Most Significant Byte	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.
NAT	*See* Network Address Translation.
netmask	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation	A technique by which several hosts share a single IP address for access to the Internet.
packet	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
PPP	*See* Point-to-Point Protocol.
PPP over Ethernet	PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPTP	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
PSTN	Public Switched Telephone Network.
Point-to-Point Protocol	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
RFC	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org.
RIP	*See* Routing Information Protocol.
router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Routing Information Protocol	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
subnet mask	*See* netmask.
UPnP	*See* Universal Plug and Play.
Universal Plug and Play	UPnP. A networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.
UTP	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

WAN	*See* wide area network.
wide area network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
Windows Internet Naming Service	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.
WINS	*See* Windows Internet Naming Service.

Index